MARSH JLT SPECIALTY

Cyber Risk Management in the US Renewable Energy Sector

As leaders of the US clean energy transition, renewable energy organizations are high-profile targets for hackers and other cyber-attackers motivated to disrupt critical US infrastructure for either political or competitive reasons. Their rapidly expanding footprints, complex supply chains, and diverse and distributed infrastructure make renewable energy organizations especially prone to operational disruptions from cyber-attacks.

In addition, renewable energy companies' increasing asset distribution and reliance on digital solutions also heighten the risk of cyber events.

With cyber-attacks increasing in frequency and severity, it is no surprise that **65% of organizations in the energy sector** say they are challenged to keep pace with their evolving cyber risks. Compounding the challenge, renewable energy companies are now subject to cyber endorsements under their property policies that limit or exclude physical damage if arising out of a cyber event.

Cyber Event Scenarios and Impact

Renewable energy organizations are most likely to suffer losses through ransomware and operational disruption, which can contribute to lost earnings, incident response costs and other extra expenses, liability for failure to fulfill contractual obligations, and regulatory investigations and fines.

These attacks can also have a significant physical impact, including infrastructure damage, control system outages, property destruction, and bodily harm, as well as resulting in financial losses.

To combat these emerging cyber threats, the renewable energy sector requires a forward-looking view of cyber risk management.

Helping You Understand, Measure, and Manage Cyber Risk

As the leading broker to the renewable energy industry, Marsh is well-positioned to help you understand your cyber risk and measure the financial impact of potential cyber incidents. Our team of renewable industry cyber specialists will help you manage your risk through consultative advisory and optimal risk transfer solutions. We can help you design easy-to-understand insurance protection that responds when needed and is tailored to your specific needs.

MARSH

Understand Cyber Risk

- Consultation with your risk management, information security, legal, and human resources teams.
- Gap analysis of your insurance program to assess your coverages and identify any gaps or overlaps related to cyber events.
- Provision of cybersecurity advisory services for your board of directors.
- Review of your enterprise cybersecurity policy.
- Assessment of your cybersecurity program maturity and program reviews.
- Assessment of your organization's and your vendors' cyber threat environment.
- Development and continuous monitoring of your third-party and vendor risk management program.
- Detailed briefings for you of industry-specific cybersecurity threat intelligence on threats from nation-states, organized crime, terrorist actors, hacktivists, and others.

Measure Your Cyber Exposures

- Evaluate your financial exposures for insurable and non-insurable risks through scenario-based, financial stress testing.
- Develop models tailored to your organization, providing empirical measurement of network interruption, data breach, SCADA/ICS, and property damage risks at both the business unit and enterprise levels.
- Provide frequency and severity for both cyber-attacks and system failures in forward-looking models.
- Connect risk evaluation to your broader enterprise risk and board reporting measures.
- Evaluate the most efficient and optimal risk transfer strategies and investment in control frameworks.

Manage Your Cyber Risk

- Secure enhanced business interruption coverage that responds to network attacks, with or without physical damage.
- Secure specific renewable industry sector regulatory risk protection.
- Limit war exclusions and other language that could preclude coverage for cyberterrorism.
- Obtain protection for network attacks against or failures of both enterprise systems and industrial control systems.
- Protect against contractual liability for failing to supply electricity.
- Demonstrate a level of risk management maturity that differentiates your projects from others.
- Help you develop operational procedures based on industry best practices.
- Test the performance of your cybersecurity controls.
- Optimize and accelerate your claims recovery in the event of a cyber incident.

Marsh Cyber Practice by the Numbers

- Placing more than **$1 billion** in global premiums annually
- Serving more than **6,300** cyber and E&O clients
- **230 specialist** cyber professionals worldwide
- Leader of **25 year-old** cyber insurance market
- ***Broker Team of the Year ($500M+)*** Business Insurance US awards 2019
- ***Cyber Broker of the Year*** Advisen 3-time Winner

To learn more, contact your Marsh representative or specialists from Marsh's Renewables Industry and Cyber Brokerage and Consulting practices.

MICHAEL KOLODNER
Managing Director,
US Renewables Industry Practice
+1 302 588 5654
michael.kolodner@marsh.com

REID SAWYER
Managing Director,
US Cyber Consulting Practice
+1 630 442 3506
reid.sawyer@marsh.com

KAITLIN UPCHURCH
Senior Vice President,
US Cyber Brokerage Practice
+1 214 934 3261
kaitlin.upchurch@marsh.com

MICHAEL GAUDET
Managing Director,
US Energy, Power & Utility Practice
+1 215 246 1226
michael.j.gaudet@marsh.com